# Developing Compliance to the Net-Ready Key Performance Parameter (NR-KPP)

LTC Tom Gaetjen, USA
J6I
703-692-4164

Lt Col Michael Convertino, US
J6I
703-614-3864

# Introduction

This information is offered to assist Combatant Commands, the Services, and DOD Agencies in the development of the Net-Ready Key Performance Parameter (NR-KPP) for Initial Capability Documents (ICDs), Capability Development Documents (CDDs), Capability Production Documents (CPDs) and Information Support Plans (ISPs).

The Net-Ready KPP consists of 4 pillars: Integrated Architecture Products, and Compliance with the Net Centric Operations and Warfare Reference Model (NCOW RM), Key Interface Profiles (KIPs), and Information Assurance (IA) requirements. The first section provides the set of integrated architecture products required for the NR-KPP, which includes selected operational, systems and technical views. Descriptions of the views are provide to aid developers of the various views. Other architecture views may be required to fully develop and assess a given capability.

The second section includes the remaining interoperability products of the NR-KPP: the Net Centric Operations and Warfare Reference Model (NCOW RM), Key Interface Profiles (KIPs), Information Assurance (IA), and Levels of Information System Interoperability (LISI) Profile. Guidance is also provided to ensure compliance with the mandated models, profiles, and certification processes.

The DOD Architecture Framework V1.0, CJCSI 6212.01C, DODD 4630.5, and

# Net-Ready KPP

| Net-Ready KPP | Threshold (T) | Objective (O) |
|---|---|---|
| All activity interfaces, services, policy-enforcement controls, and data-sharing of the NCOW-RM and GIG-KIPs will be satisfied to the requirements of the specific integrated architecture products (including data correctness, data availability and data processing*), and information assurance accreditation, specified in the threshold (T) and objective (O) values. | 100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements designated as enterprise-level or critical in the Joint integrated architecture**. | 100% of interfaces; services; policy-enforcement controls; and data correctness, availability and processing* requirements in the Joint integrated architecture. |

# Net-Ready KPP 4 Pillars

Supporting Architecture Products

NCOW RM Compliance

Key Interface Profiles Compliance

Information Assurance (IA) Compliance

# Migration Timeline to the NR-KPP

**Today - IER Based I KPP**

**Current Interoperability KPP (I KPP) Centers around one DOD Architectural Operational View (OV-3) that contains Information Exchange Requirements (IER)**

**FY04 - FY 06 NET READY KPP**

**Net Centric Operations Warfare NCOW Reference Model Compliance**

**Integrated Architecture**

***Applicable KIPs**

**Information Assurance**

Measurable and Testable Net-Ready KPP

**FY06 NET READY KPP**

- **Net Centric Operations Warfare (NCOW) Reference Model Compliance**
- **Integrated Architecture**
- **Key Interface Profiles (KIPs)**
- **Information Assurance**

Measurable and Testable Net-Ready KPP

**FY06 and Beyond - NET READY**

**Net Ready approach centers on Central network:**

**•Focus on organizational contributions and consumption of information**

**•One-to-Network paradigm**

# Principal NR-KPP Products Matrix

| Document | Net-Ready Key Performance Parameter Products | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Supporting Architecture Products | | | | | | | | | | | | | | | |
| | AV-1 | OV-1 | OV-2 | OV-3 | OV-4 | OV-5 | OV-6C | SV-1 | SV-4 | SV-5 | SV-6 | TV-1 | NCOW RM Correlation | KIP Compliance | IA Compliance | LISI Profile |
| ICD | | X | | | | | | | | | | | X | | | |
| CDD | X | | X | | X | X | X | | X | X | X | X | X | X | X | X Basic |
| CPD | X | | X | | X | X | X | | X | X | X | X | X | X | X | X Complete |
| CRD | | X | | 1 | | 2 | | | | | | | 2 | 2 | 2 | |
| ISP | 3 | 3 | 3 | | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | X Complete |

Note: X= Required
(1) Old/Legacy CRDs Updates
(2) New CRDs
(3) ACAT, Non-ACAT and Fielded Systems. NR KPP products produced for the CDD and CPD will be used in the ISP

# Overview & Summary Information, AV-

- **Architecture Project Identification**
  - -- **Name**
  - -- **Architect**
  - -- **Organization Developing the Architecture**
  - -- **Assumptions and Constraints**
  - -- **Approval Authority**
  - -- **Date Completed**
  - -- **Level of Effort and Projected and Actual Costs to Develop the Architecture**
- **Scope: Architecture View(s) and Products Identification**
  - -- **Views and Products Developed**
  - -- **Time Frames Addressed**
  - -- **Organizations Involved**
- **Purpose and Viewpoint**
  - -- **Purpose, Analysis, Questions to be Answered by Analysis of the Architecture**
  - -- **From Whose Viewpoint the Architecture is Developed**
- **Context**
  - -- **Mission**
  - -- **Doctrine, Goals, and Vision**
  - -- **Rules, Criteria, and Vision**
  - -- **Tasking for Architecture Project and Linkages to Other Architectures**
- **Tools and File Formats Used**
- **Findings**
  - -- **Analysis Results**
  - -- **Recommendations**

**Figure 3-1. Overview and Summary Information (AV-1)**

# Integrated Dictionary (AV-2)

**Integrated Dictionary: Definitions of all terms used in all products**

| | Entity | Definition and Remarks |
|---|---|---|
| 1 | **ACTION** | ***An activity***, such as an IDEF0 activity or a war fighting task. |
| 2 | **ACTIVITY-MODEL** | ***A representation of the interrelated functions of a system.*** Usually an IDEF0 activity model. |
| 3 | **AGREEMENT** | ***An arrangement between parties***, such as an IEEE standard or memorandum of agreement. |
| 4 | **ARCHITECTURE** | ***The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.*** Architectures can be operational, systems, technical, organizational, functional, AS-IS, TO-BE, or any other architecture. |
| 5 | **CAPABILITY** | ***An ability to achieve an objective.*** Examples include MOEs, MOPs, and technical performance parameters. |
| 6 | **CONCEPTUAL-DATA-MODEL** | ***A structured graphical and textual representation of concepts and knowledge within an activity.*** A description of how data are organized and how that organization reflects the information structure of a problem domain. Can describe complex (such as a database) or simple (such as a packet) data structures. Often an IDEF1X data model [FIPS 184 1993]. |

# High Level Operational Concept Graphic

Figure 4-2. Joint Task Force Concept of Operations (OV-1)

# Operational Node Connectivity Description

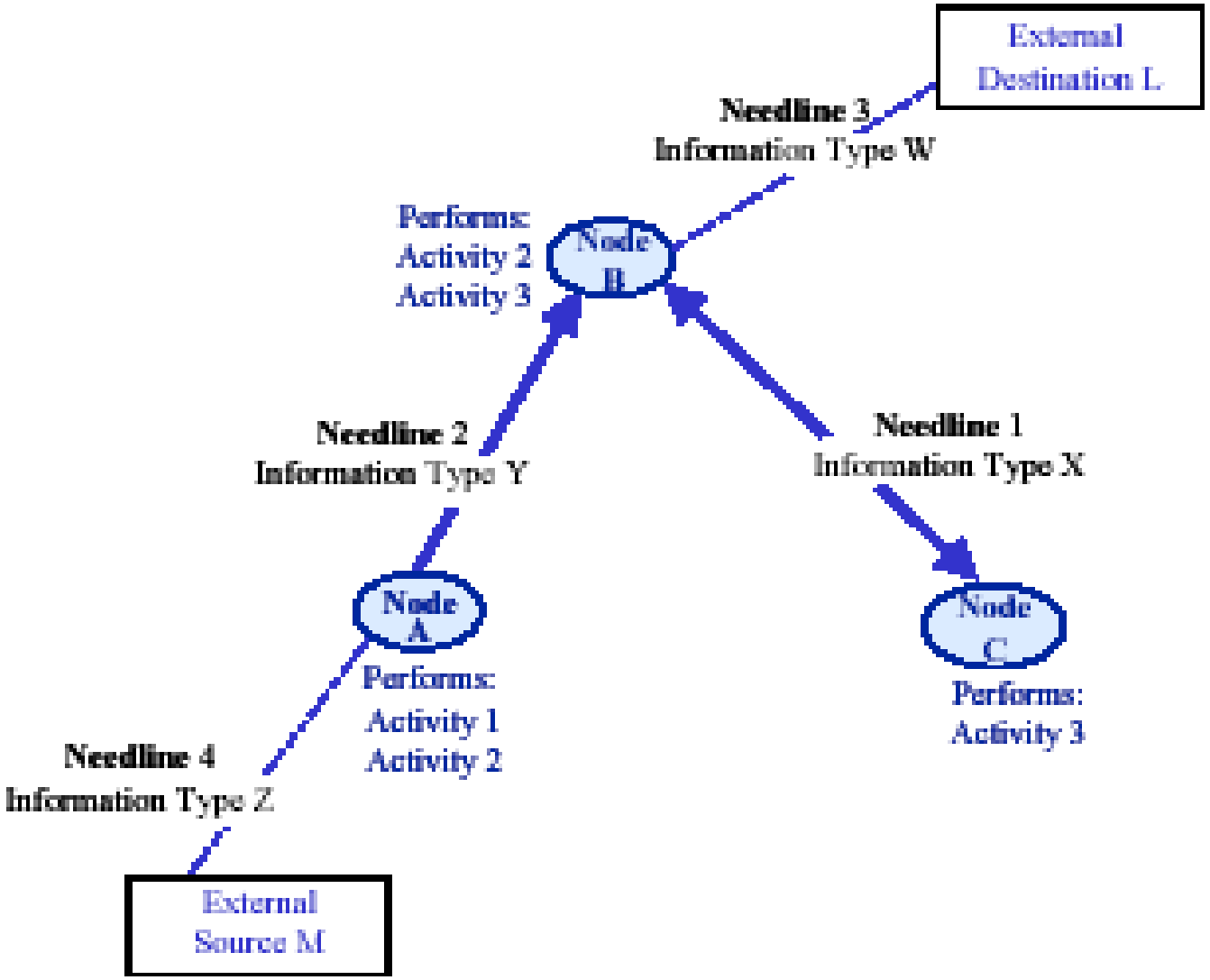



Figure 4-4. Operational Node Connectivity Description (OV-2) Template

# Operational Information Exchange Matrix

| Needline Identifier | Information Exchange Identifier | Information Element Description | | | | | Producer | | Consumer | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Information Element Name and Identifier | Content | Scope | Accuracy | Language | Sending Op Node Name and Identifier | Sending Op Activity Name and Identifier | Receiving Op Node Name and Identifier | Receiving Op Activity Name and Identifier |

| Needline Identifier | Information Exchange Identifier | Nature of Transaction | | | | | Performance Attributes | | Information Assurance | | | | Security | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Mission/Scenario UJTL or METL | Transaction Type | Triggering Event | Interoperability Level Required | Criticality | Periodicity | Timeliness | Access Control | Availability | Confidentiality | Dissemination Control | Integrity | Accountability | Protection (Type Name, Duration, Date) | Classification | Classification Caveat |

Figure 4-8. Operational Information Exchange Matrix (OV-3) – Template

# Organizational Relationships Chart, O

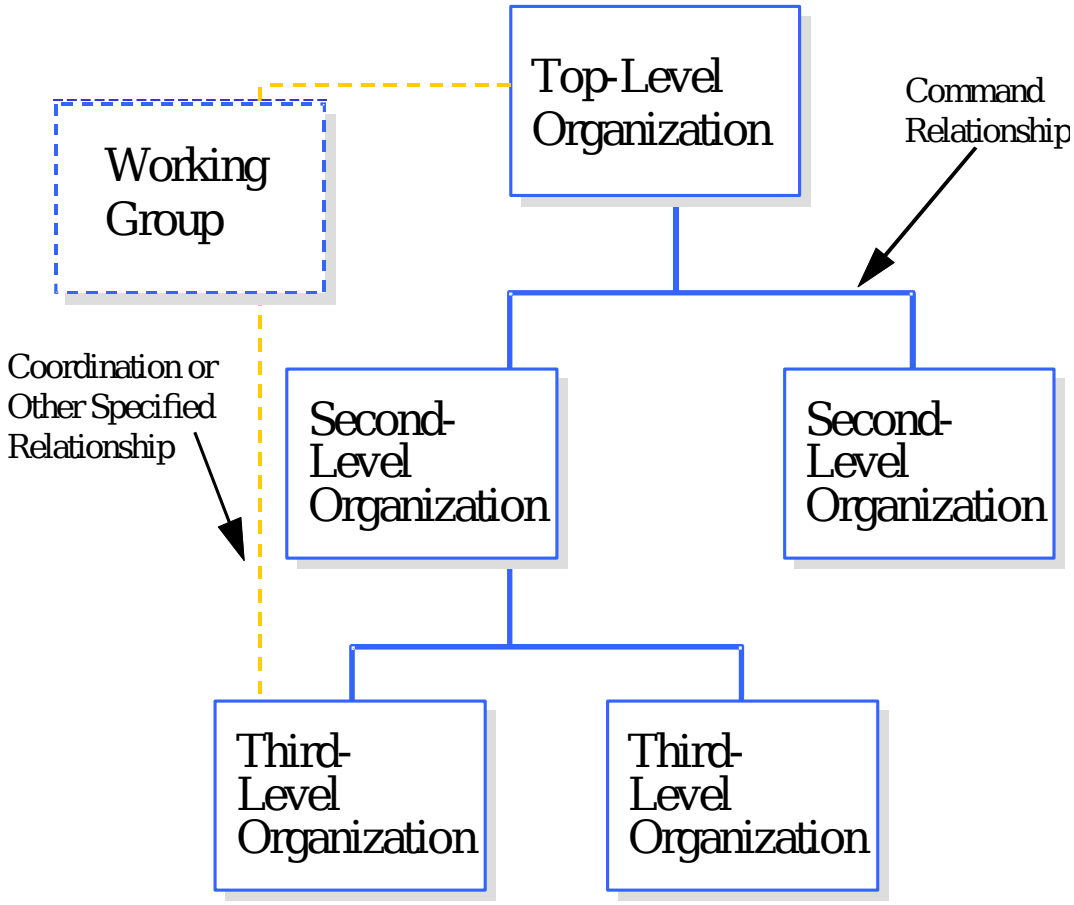
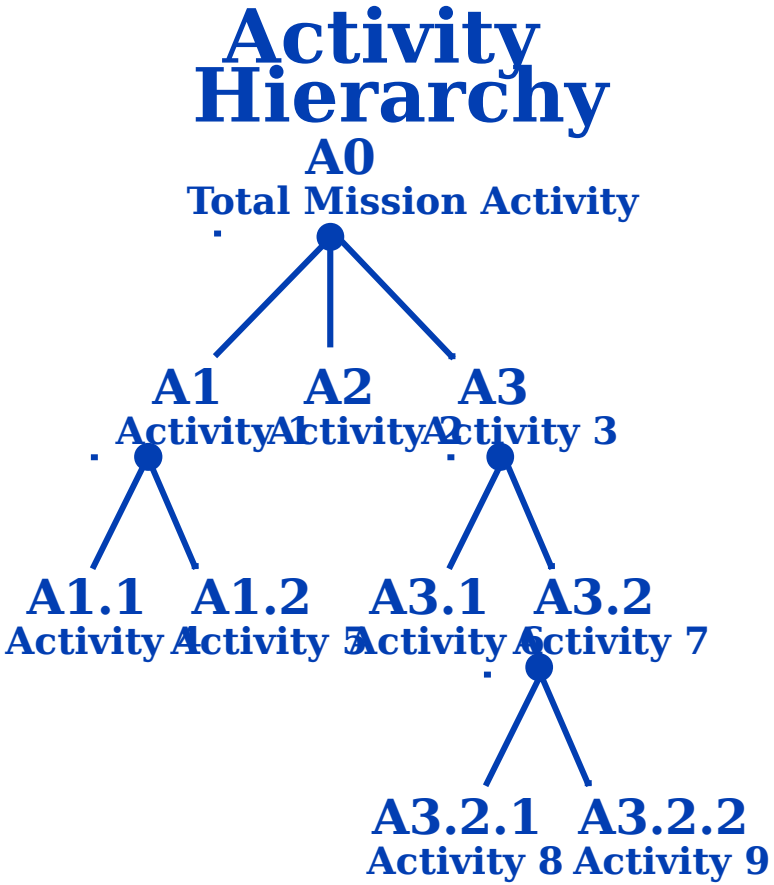



**Figure 4-11. Organizational Relationships Chart (OV-4) - Template**

# rational Activity Hierarchy Chart and Operati Activity Diagram (OV-5)



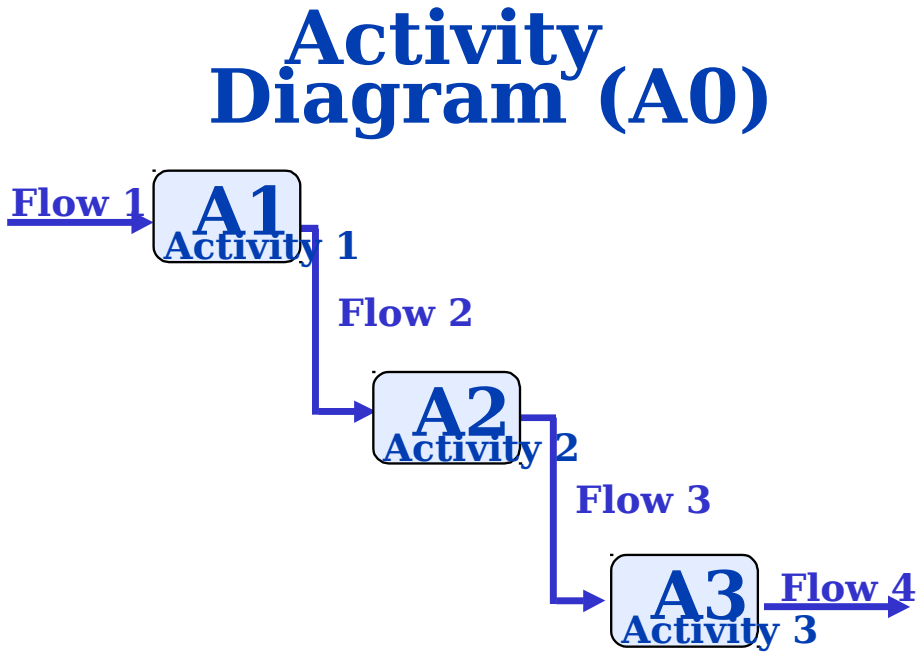




**Figure 4-14. Operational Activity Hierarchy Chart and Operational Activity Diagram (OV-5) - Templates**

# Operational Event-Trace Description, OV

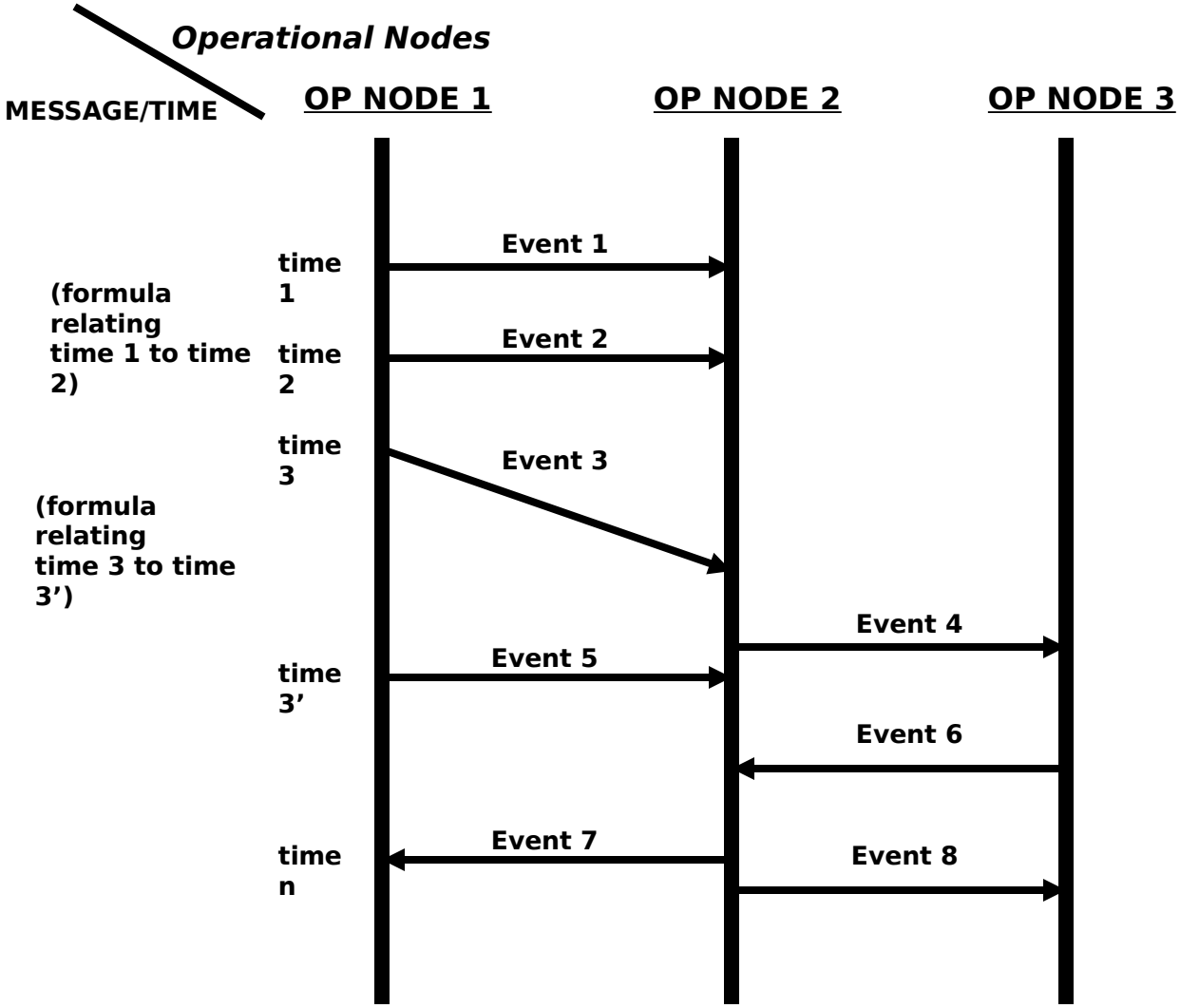
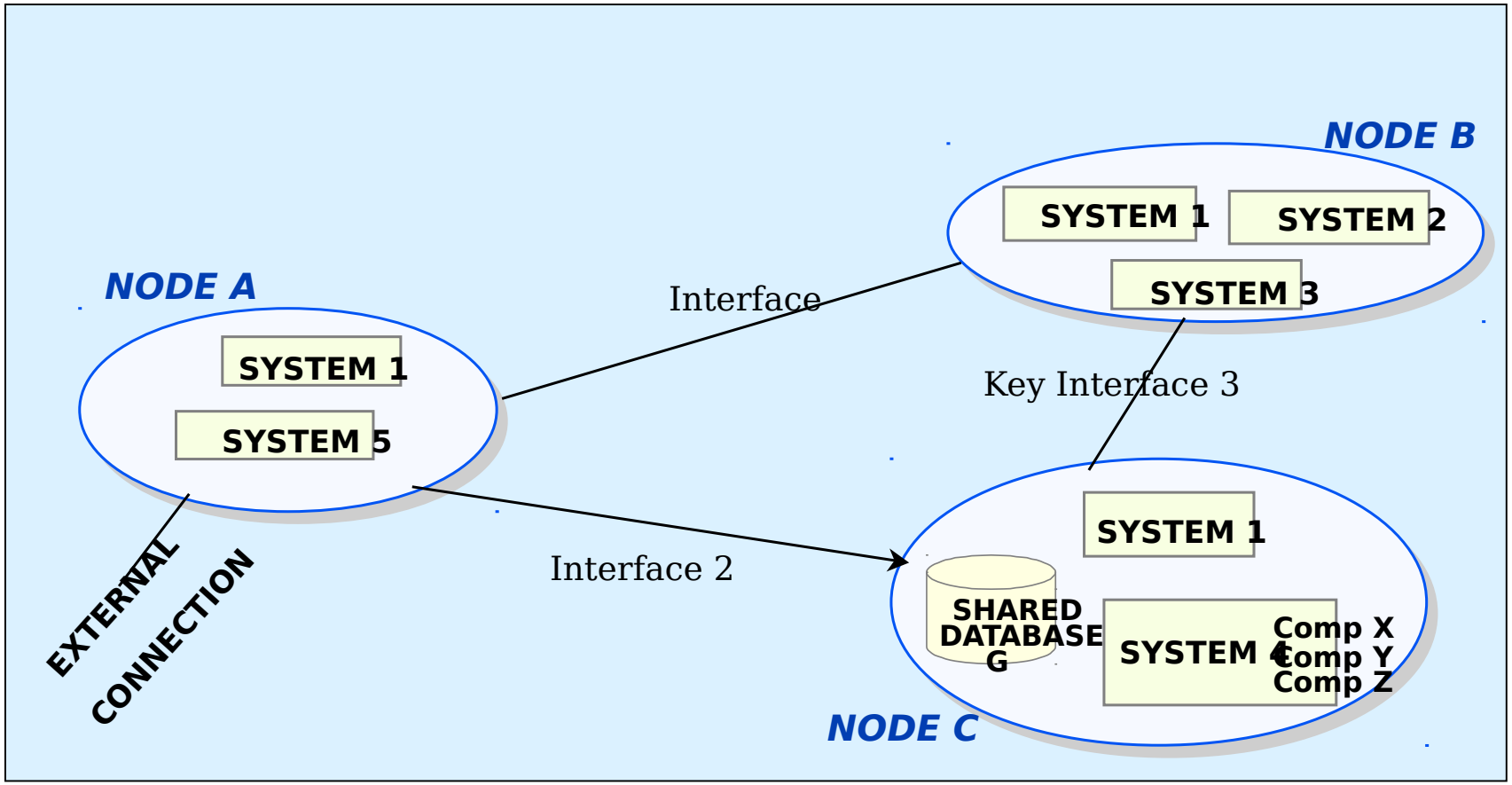



**Figure 4-27. Operational Event-Trace Description (OV-6C) – UML-Type Template**

# Systems Interface Description, SV-1



# Systems Functionality Description, SV-

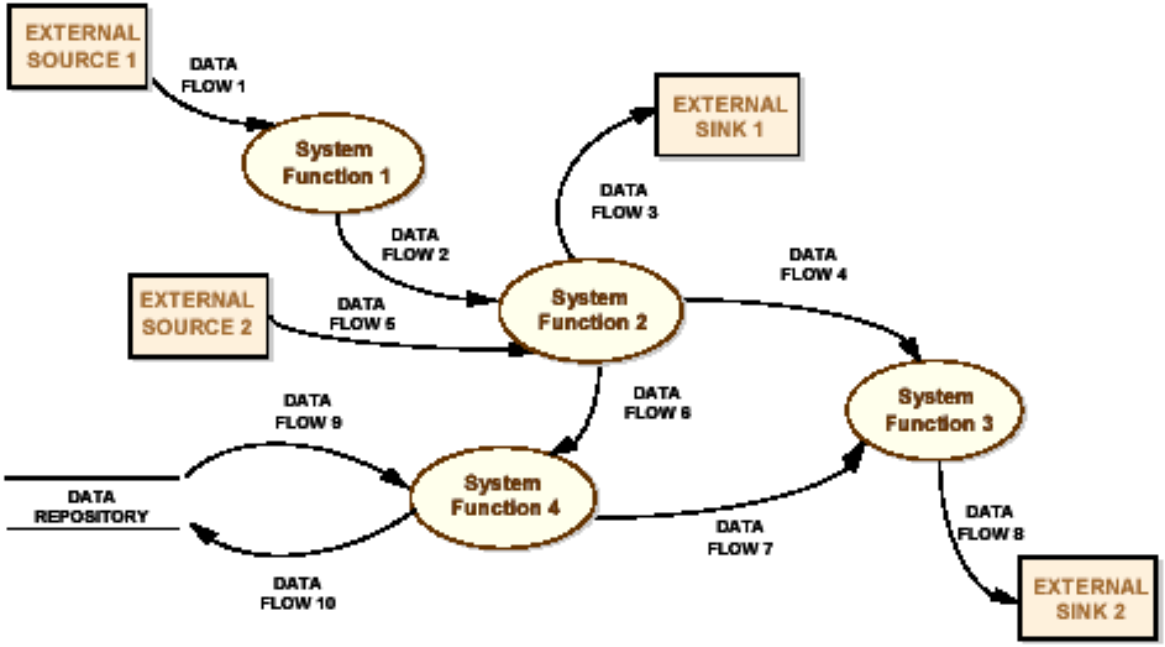



Figure 5-15. Systems Functionality Description (SV-4) – Template (Data Flow Diagram)

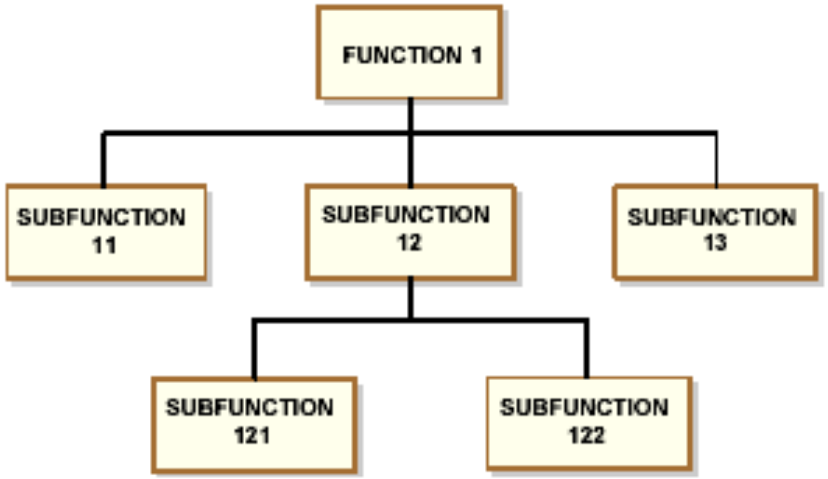
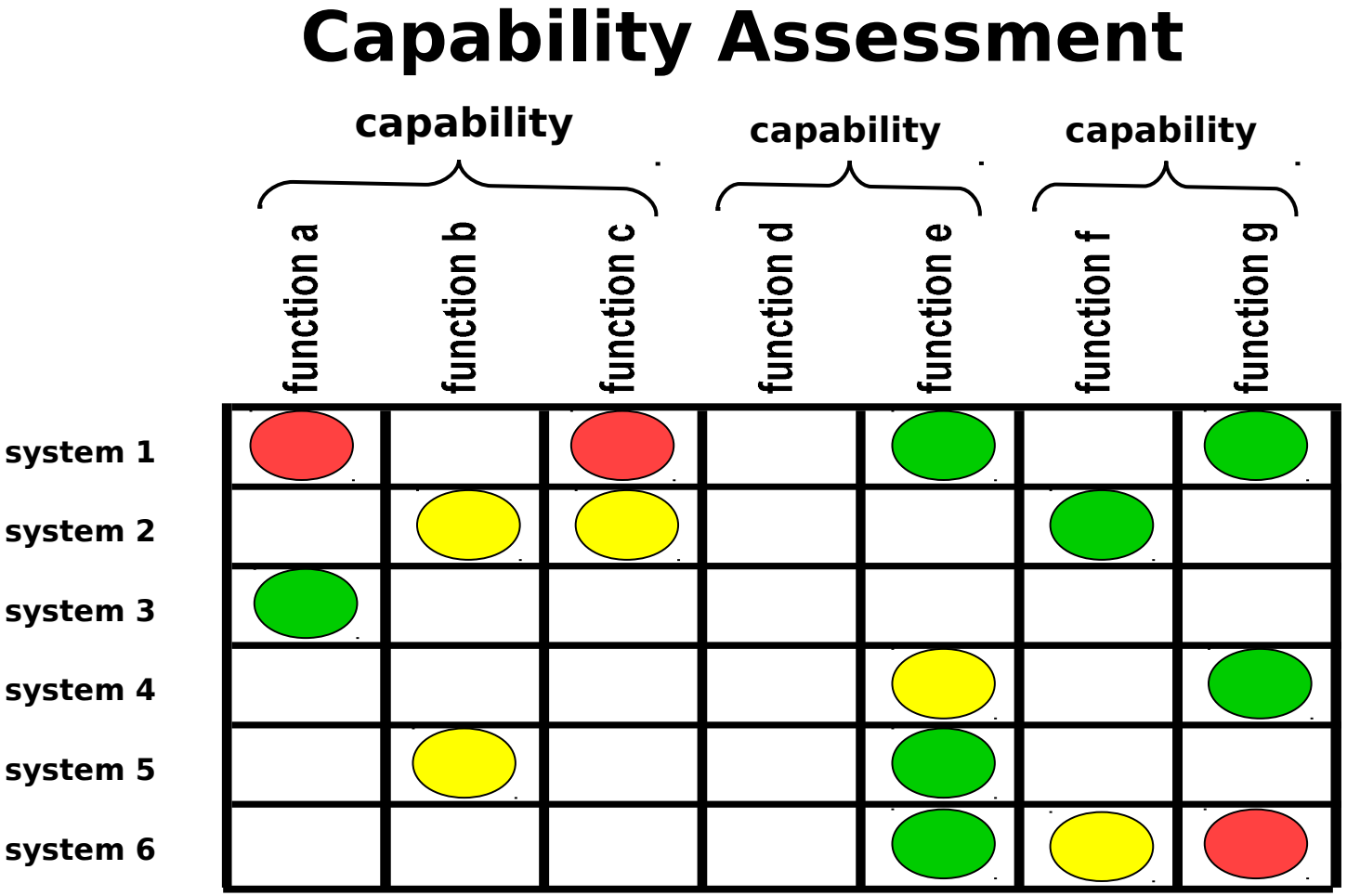



Figure 5-14. Systems Functionality Description (SV-4) – Template (Functional Decomposition)

# Operational Activity to Systems Function Traceability Matrix, SV-5



# Systems Data Exchange Matrix, SV-6

| Interface Identifier | Data Exchange Identifier | Data Description | | | | | | Producer | | Consumer | | Nature of Transaction | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| System Interface Name and Identifier | System Data Exchange Name and Identifier | Data Element Name and Identifier | Content | Format Type | Media Type | Accuracy | Units of Measurement | Data Standard | Sending System Name and Identifier | Sending System Function Name and Identifier | Receiving System Name and Identifier | Receiving System Function Name and Identifier | Transaction Type | Triggering Event | Interoperability Level Achieved | Criticality |

| Interface Identifier | Data Exchange Identifier | Performance Attributes | | | | Information Assurance | | | | | | Security | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| System Interface Name and Identifier | System Data Exchange Name and Identifier | Periodicity | Timeliness | Throughput | Size | Access Control | Availability | Confidentiality | Dissemination Control | Integrity | Non-Repudiation Producer | Non-Repudiation Consumer | Protection (Type Name, Duration, Date) | Classification | Classification Caveat | Releasability | Security Standard |

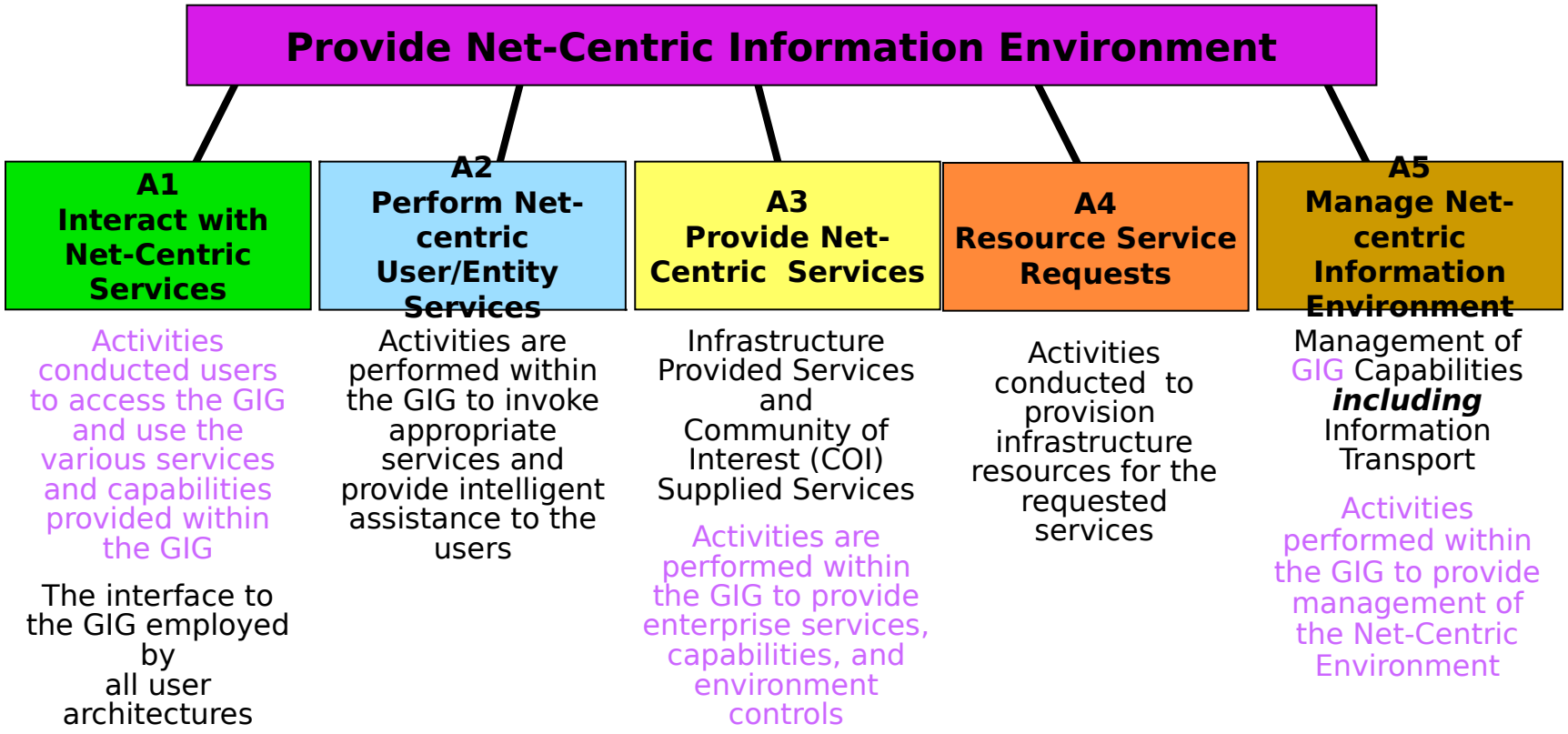
Figure 5-25. Systems Data Exchange Matrix (SV-6) – Template

# Technical Standards Profile, TV-1

**Table 6-1. Technical Standards Profile (TV-1) Template**

| JTA Service Area | Service | JTA Standard and Source Document |
|---|---|---|
| Information-Processing Standards | Higher Order Languages | |
| | Software Life-Cycle Process | |
| | Geospatial Data Interchange | |
| | Motion Imagery Data Interchange - Video | |
| | Distributed-Object Computing | |
| Information-Transfer Standards | Data Flow Network | |
| | Command and Control Information (C2I) Network | |
| | Physical Layer | |
| | Network Interface | |
| | Layer Management | |
| | File Transfer Standards | |
| | Remote Terminal Standards | |
| | Network Time Synchronization Standards | |
| | Web Services Standards | |
| | Connectionless Data Transfer | |
| | Transport Services Standards | |
| Information Modeling, Metadata, and Information Exchange Standards | Activity Modeling | |
| | Data Modeling | |
| | Object-Oriented Modeling | |
| Human Computer Interface | Mandates | |
| Infrastructure Standards | Password Security | |
| | Application Software Entity Security Standards | |
| | Virtual Private Network Service | |
| | Intrusion Detection Service | |
| | Human-Computer Interface Security Standards | |

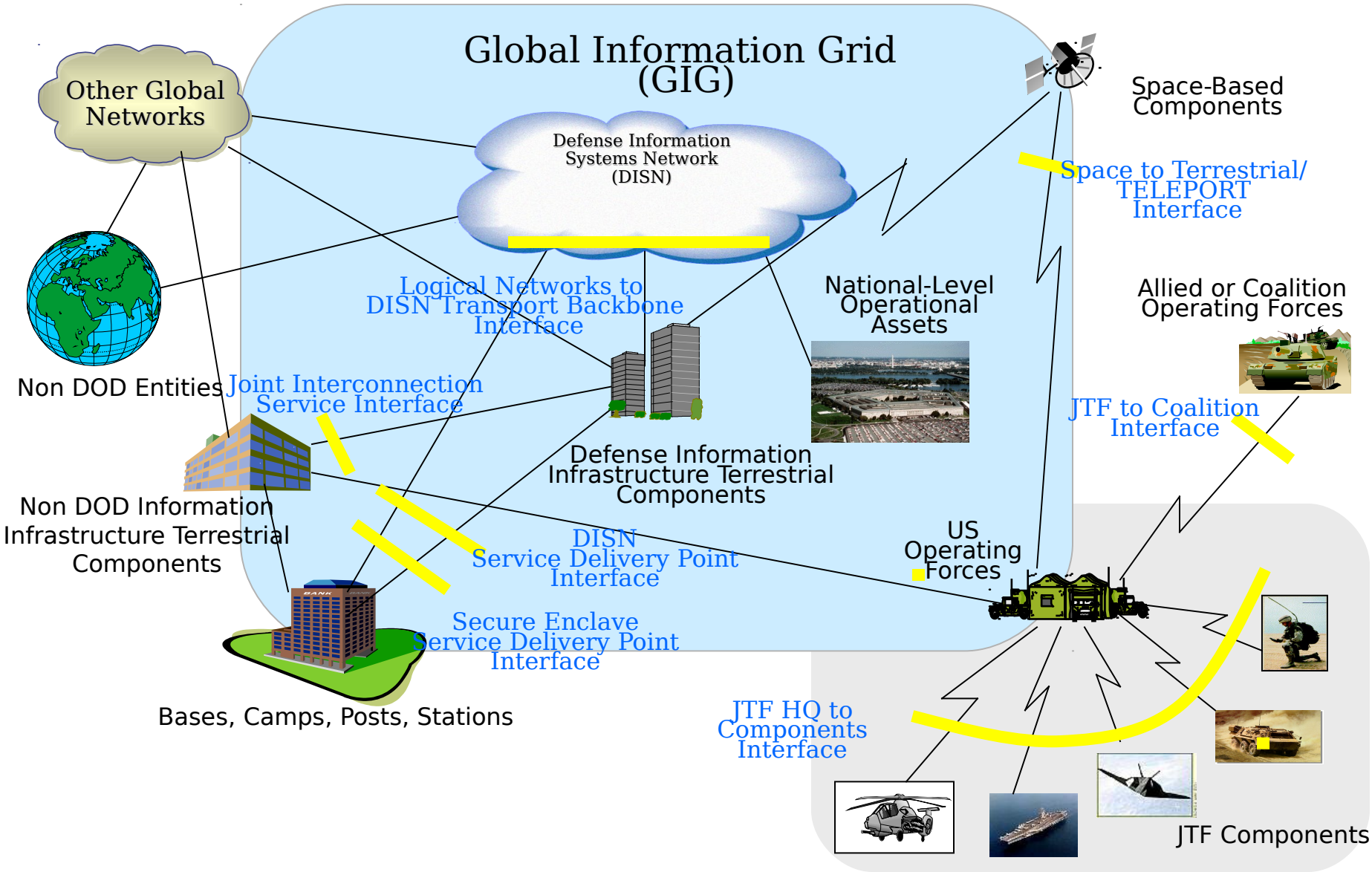
# Net-Centric Operations & Warfare Reference Model


Provide Net-Centric Information Environment
A1
Interact with Net-Centric Services
Activities conducted users to access the GIG and use the various services and capabilities provided within the GIG
The interface to the GIG employed by all user architectures
A2
Perform Net-centric User/Entity Services
Activities are performed within the GIG to invoke appropriate services and provide intelligent assistance to the users
A3
Provide Net-Centric Services
Infrastructure Provided Services and Community of Interest (COI) Supplied Services
Activities are performed within the GIG to provide enterprise services, capabilities, and environment controls
A4
Resource Service Requests
Activities conducted to provision infrastructure resources for the requested services
A5
Manage Net-centric Information Environment
Management of GIG Capabilities ***including*** Information Transport
Activities performed within the GIG to provide management of the Net-Centric Environment

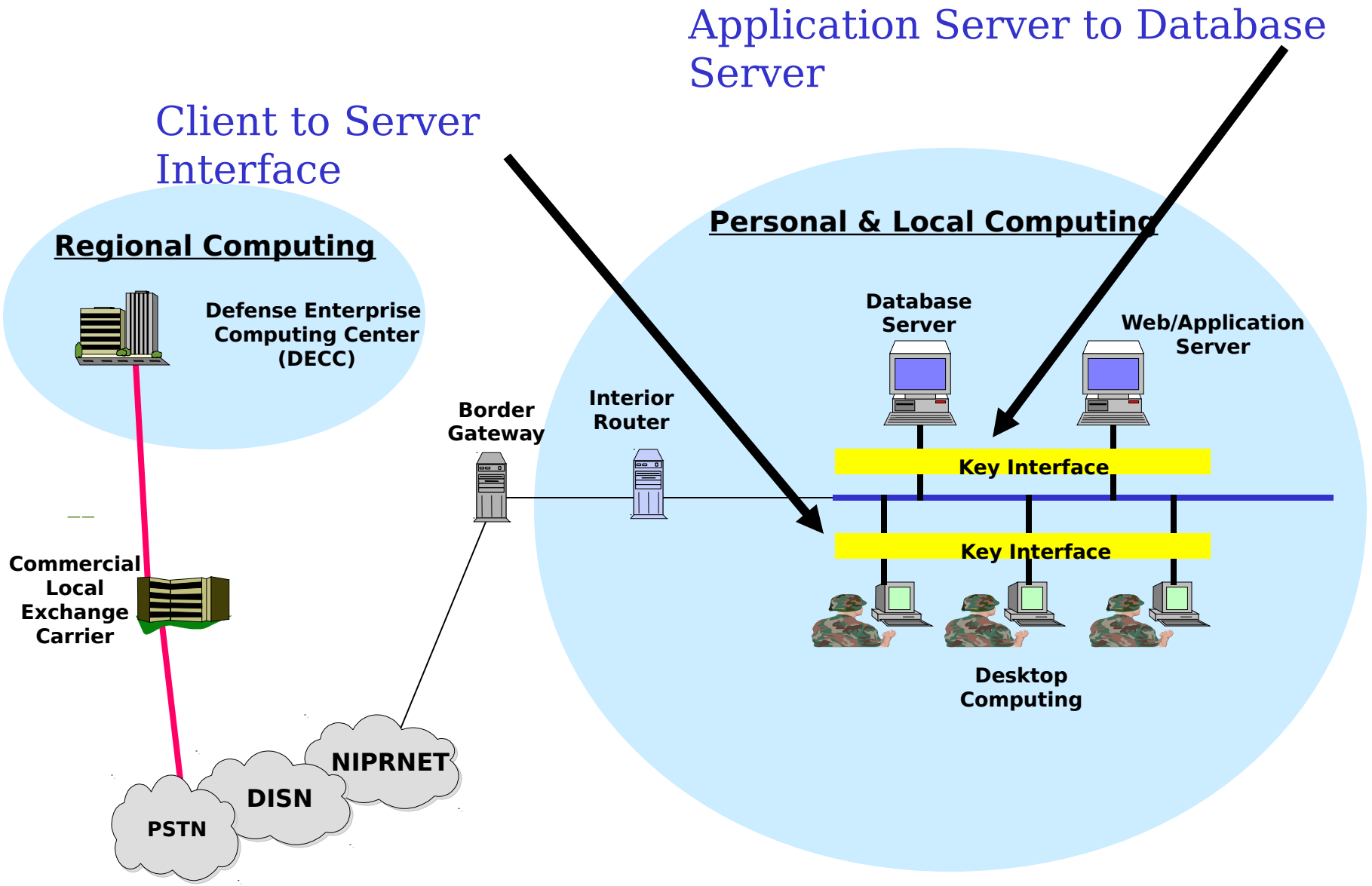
# The 17 Key Interfaces Profiles (KIPs)

1. JTF Component to JTF Headquarters
2. JTF to Coalition
3. Logical Networks to DISN Transport Backbone
4. Space to Terrestrial
5. TELEPORT
6. Client to Server
7. Application Server to Shared Data
8. DISN Service Delivery Node
9. Secure Enclave Service Delivery Node
10. Application Server to Database Server
11. Joint Interconnection Service
12. Management System to Managed Systems
13. Application to COE/CCP (NCES/GES)
14. End System to PKI
15. Information Servers to IDM Infrastructure
16. IDM to Distribution Infrastructure
17. Management System to (Integrated) Management Systems

# KIPs

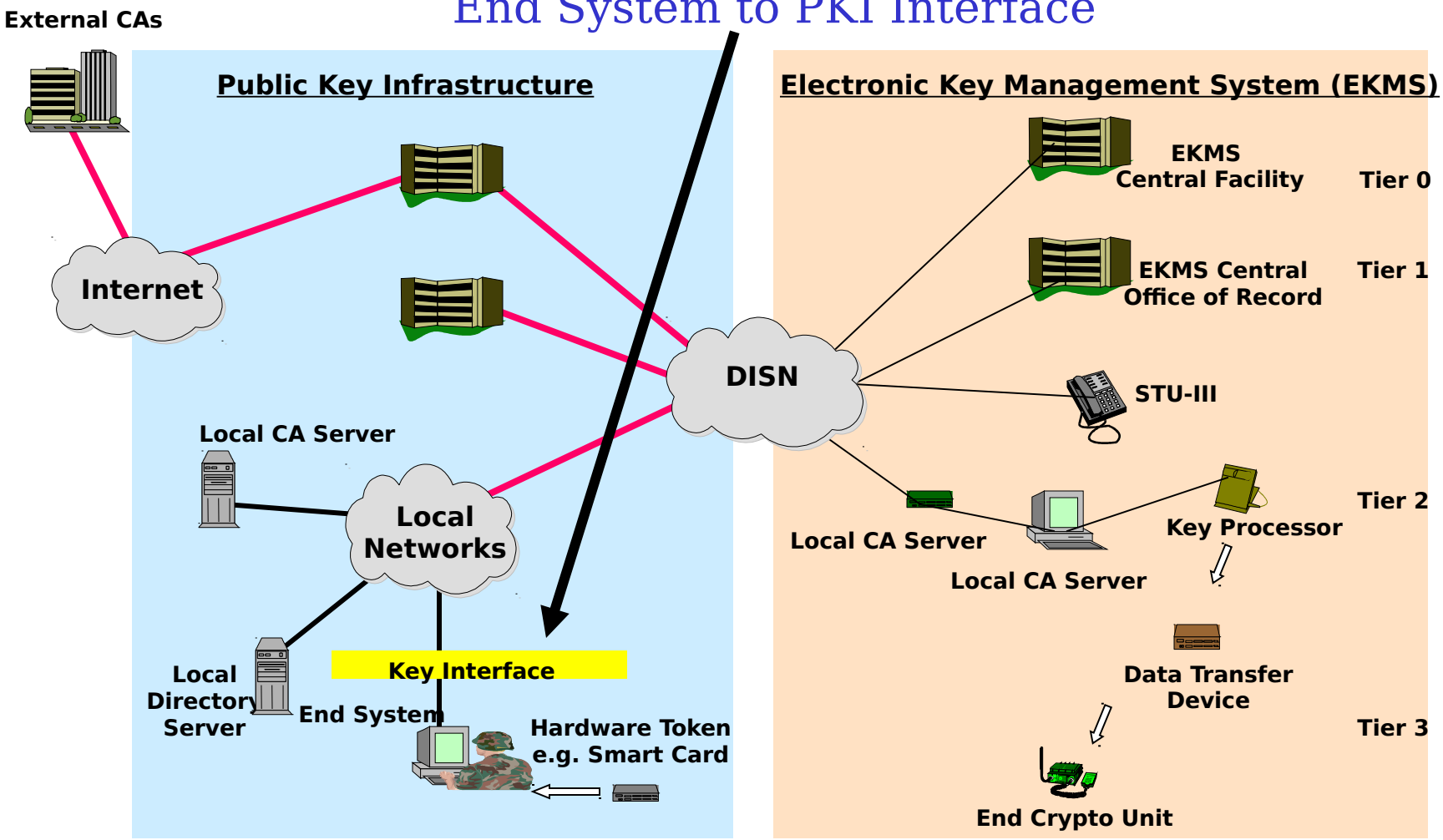

Global Information Grid (GIG)
Other Global Networks
Defense Information Systems Network (DISN)
Space-Based Components
Space to Terrestrial/ TELEPORT Interface
Logical Networks to DISN Transport Backbone Interface
National-Level Operational Assets
Allied or Coalition Operating Forces
Non DOD Entities
Joint Interconnection Service Interface
JTF to Coalition Interface
Defense Information Infrastructure Terrestrial Components
Non DOD Information Infrastructure Terrestrial Components
DISN Service Delivery Point Interface
US Operating Forces
Secure Enclave Service Delivery Point Interface
JTF HQ to Components Interface
Bases, Camps, Posts, Stations
JTF Components

# KIPs cont'd

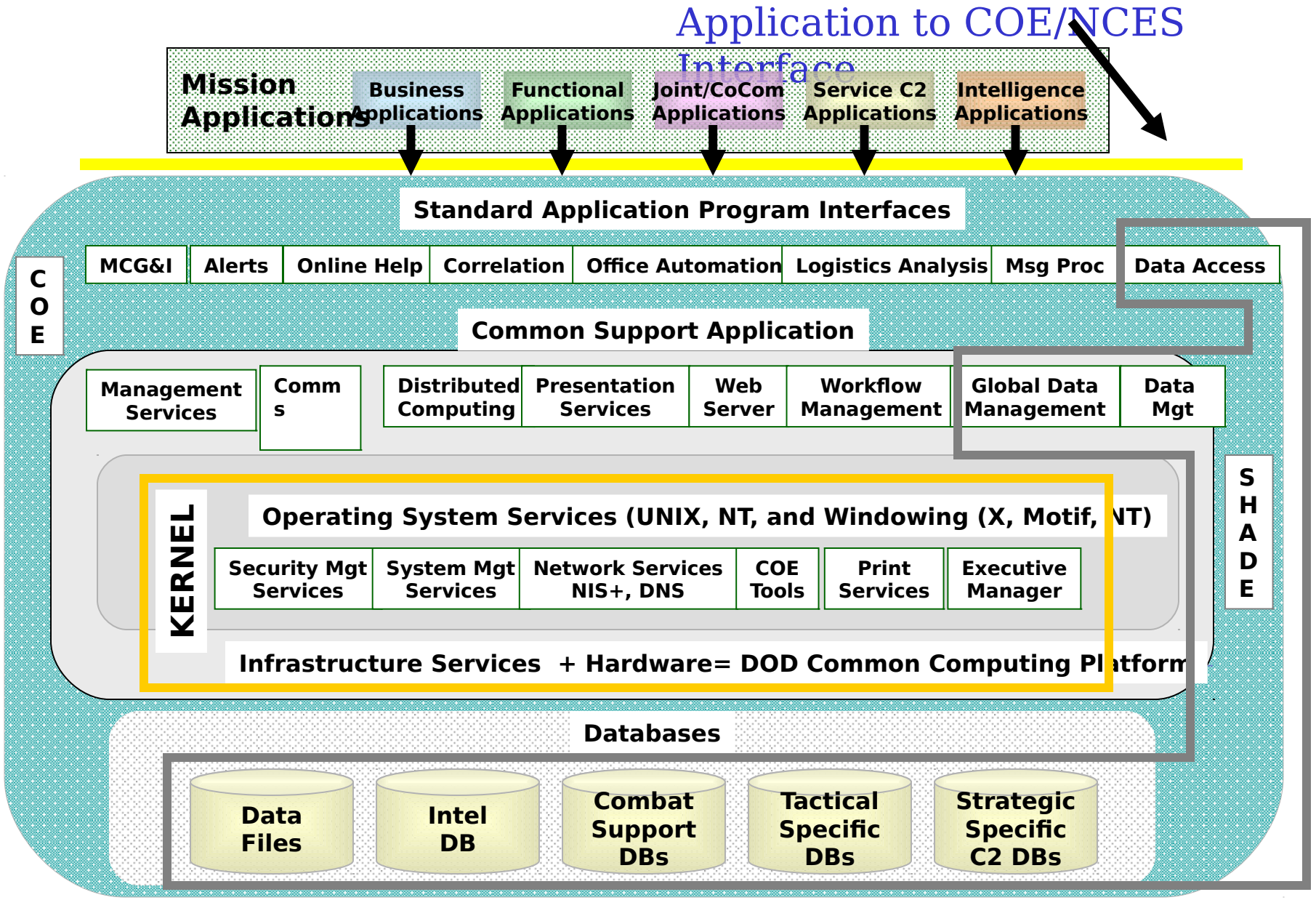

Application Server to Database Server
Client to Server Interface
Regional Computing
Defense Enterprise Computing Center (DECC)
Personal & Local Computing
Database Server
Web/Application Server
Border Gateway
Interior Router
Key Interface
Key Interface
Commercial Local Exchange Carrier
Desktop Computing
NIPRNET
DISN
PSTN

# KIPs cont'd

## End System to PKI Interface

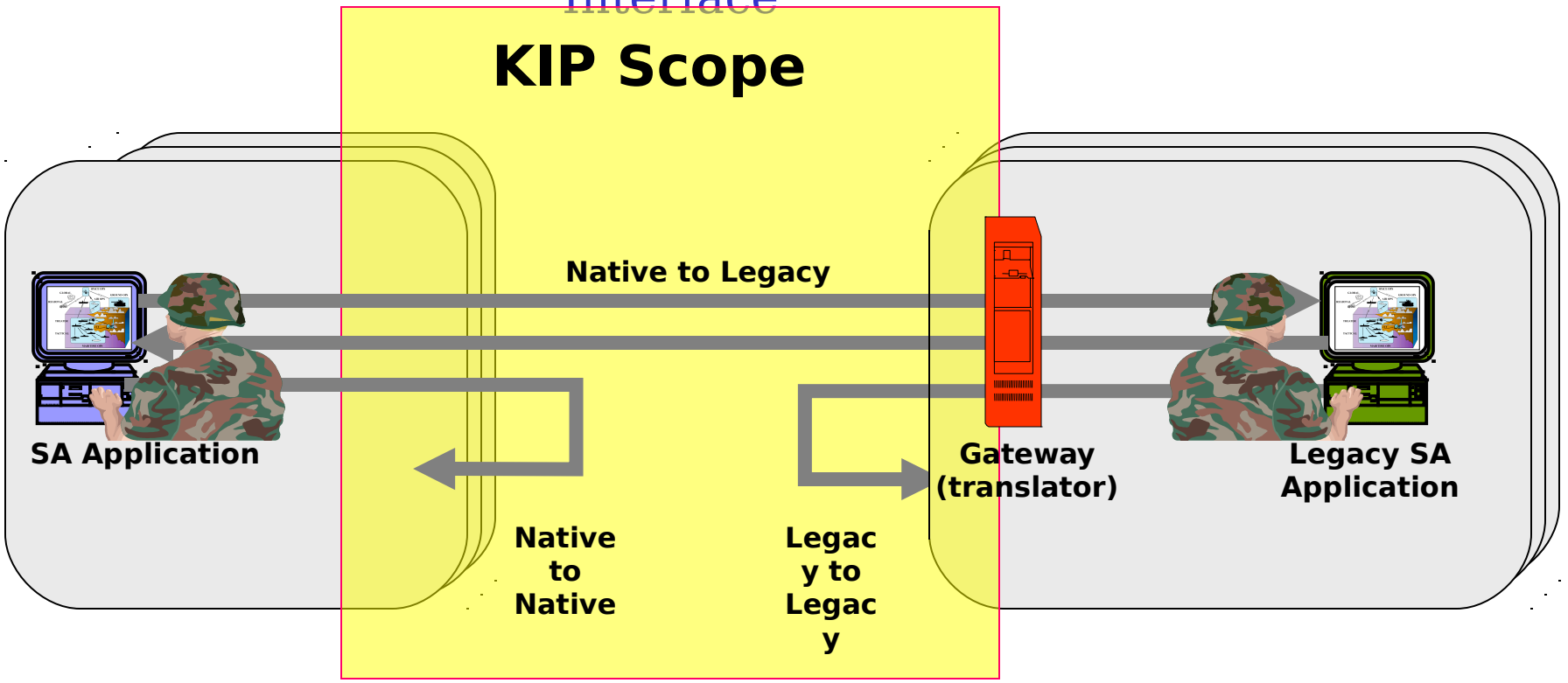


# KIPs cont'd

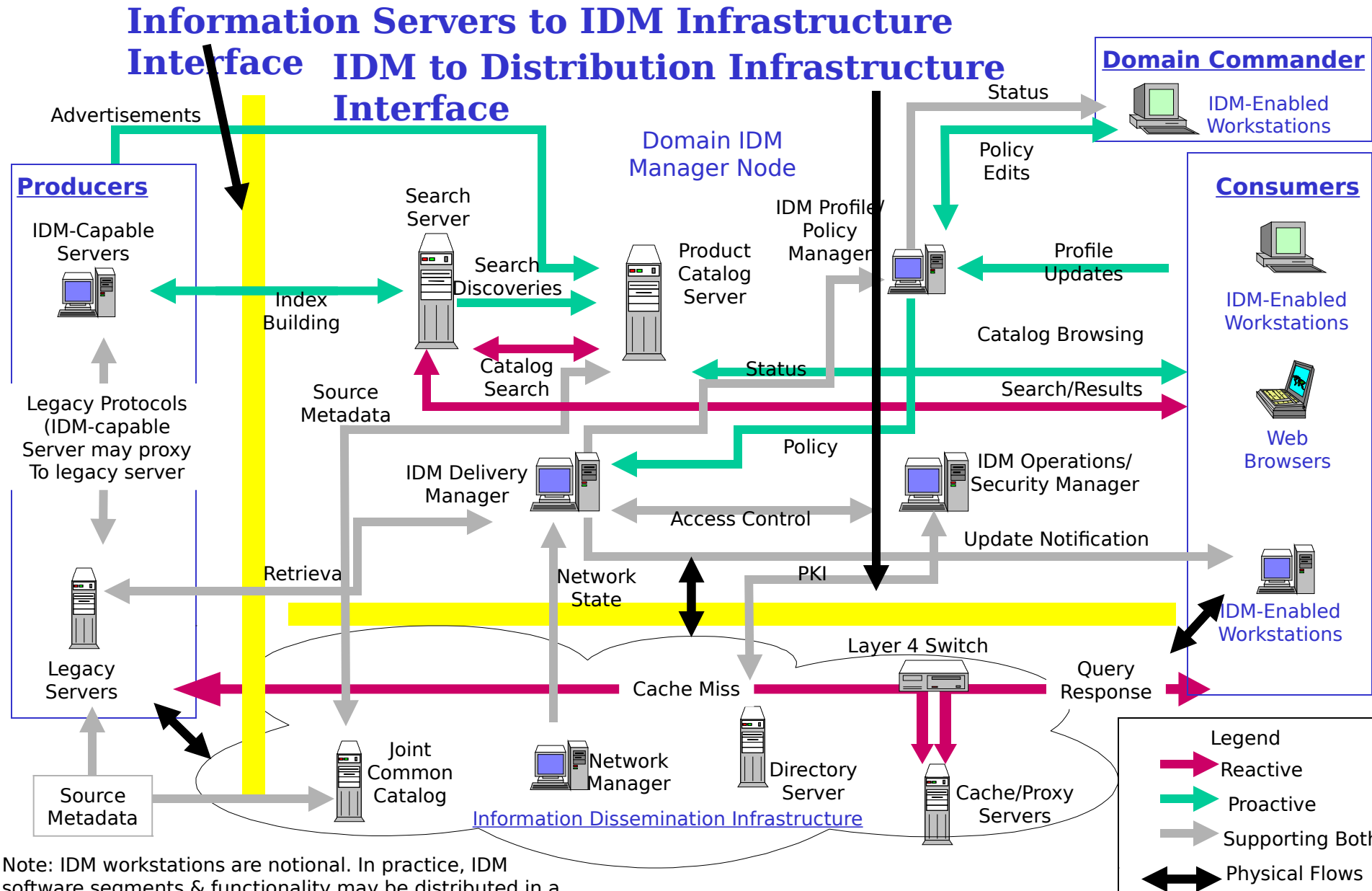

Application to COE/NCES Interface
Mission Applications
Business Applications
Functional Applications
Joint/CoCom Applications
Service C2 Applications
Intelligence Applications
Standard Application Program Interfaces
COE
MCG&I
Alerts
Online Help
Correlation
Office Automation
Logistics Analysis
Msg Proc
Data Access
Common Support Application
Management Services
Comm s
Distributed Computing
Presentation Services
Web Server
Workflow Management
Global Data Management
Data Mgt
SHADE
KERNEL
Operating System Services (UNIX, NT, and Windowing (X, Motif, NT)
Security Mgt Services
System Mgt Services
Network Services NIS+, DNS
COE Tools
Print Services
Executive Manager
Infrastructure Services + Hardware= DOD Common Computing Platform
Databases
Data Files
Intel DB
Combat Support DBs
Tactical Specific DBs
Strategic Specific C2 DBs

# KIPs cont'd

Situational Awareness Data Interoperability Interface

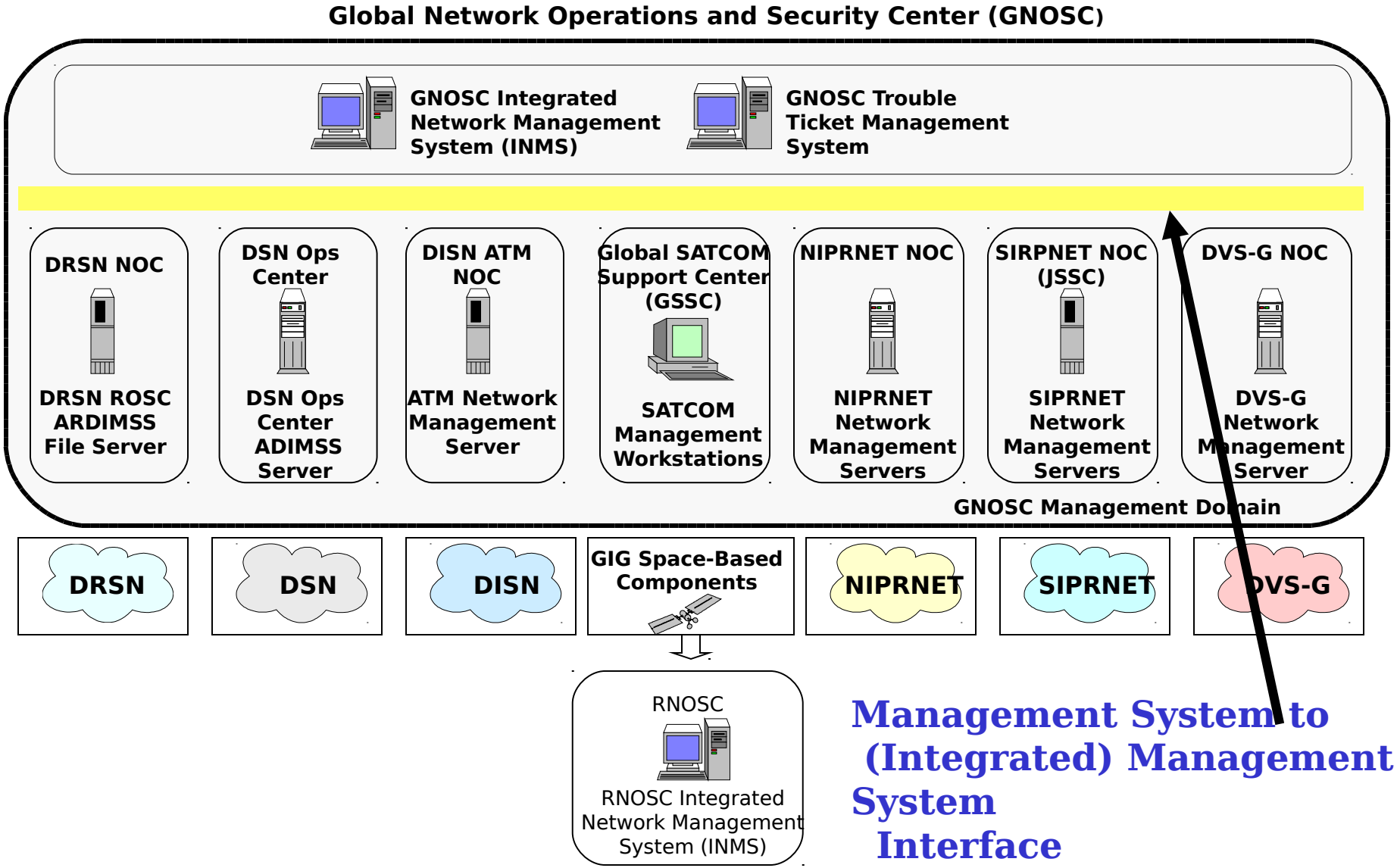


# KIPs cont'd

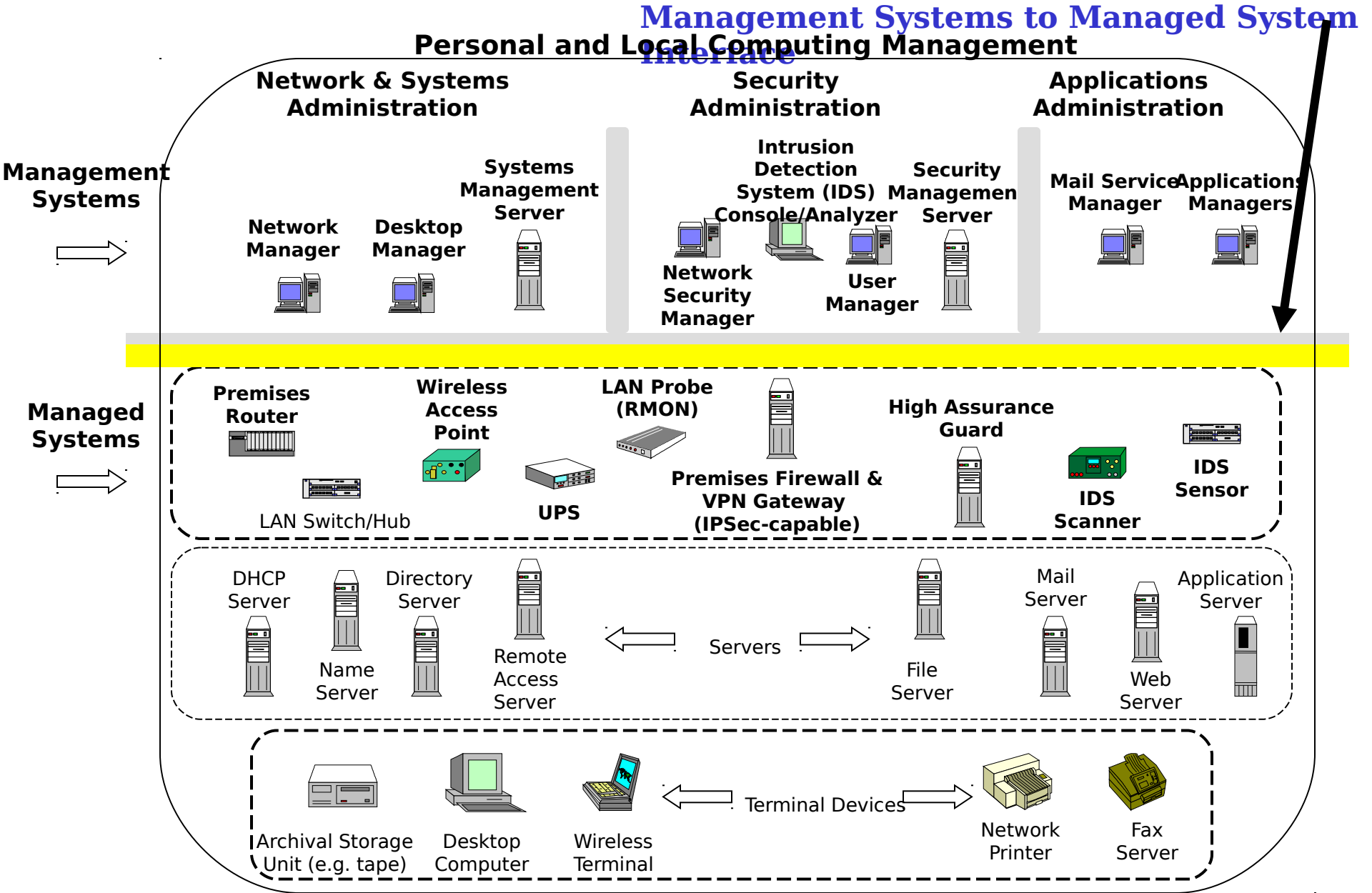



Note: IDM workstations are notional. In practice, IDM software segments & functionality may be distributed in a

# KIPs cont'd

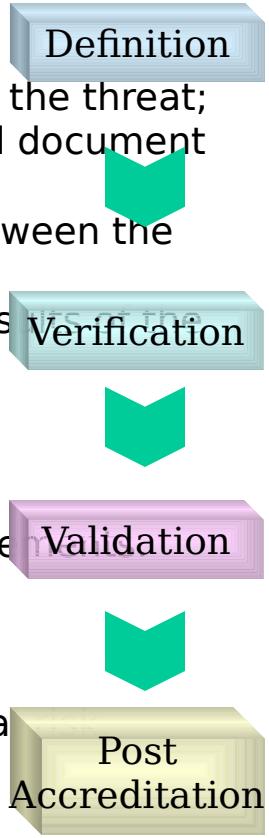

Global Network Operations and Security Center (GNOSC)
GNOSC Integrated Network Management System (INMS)
GNOSC Trouble Ticket Management System
DRSN NOC
DRSN ROSC ARDIMSS File Server
DSN Ops Center
DSN Ops Center ADIMSS Server
DISN ATM NOC
ATM Network Management Server
Global SATCOM Support Center (GSSC)
SATCOM Management Workstations
NIPRNET NOC
NIPRNET Network Management Servers
SIRPNET NOC (JSSC)
SIPRNET Network Management Servers
DVS-G NOC
DVS-G Network Management Server
GNOSC Management Domain
DRSN
DSN
DISN
GIG Space-Based Components
NIPRNET
SIPRNET
DVS-G
RNOSC
RNOSC Integrated Network Management System (INMS)
Management System to (Integrated) Management System Interface

# KIPs cont'd


Management Systems to Managed System Interface
Personal and Local Computing Management
Network & Systems Administration
Security Administration
Applications Administration
Management Systems
Network Manager
Desktop Manager
Systems Management Server
Intrusion Detection System (IDS) Console/Analyzer
Security Management Server
Network Security Manager
User Manager
Mail Service Manager
Applications Managers
Managed Systems
Premises Router
LAN Switch/Hub
Wireless Access Point
UPS
LAN Probe (RMON)
Premises Firewall & VPN Gateway (IPSec-capable)
High Assurance Guard
IDS Scanner
IDS Sensor
DHCP Server
Name Server
Directory Server
Remote Access Server
Servers
File Server
Mail Server
Web Server
Application Server
Archival Storage Unit (e.g. tape)
Desktop Computer
Wireless Terminal
Terminal Devices
Network Printer
Fax Server

# Information Assurance

The Defense Information Technology Security Certification and Accreditation Program (DITSCAP) (DODD 5200.28) process consists of the following phases:




**Phase 1, Definition**
Activities to document the system mission, environment, and architecture; identify the threat; define the levels of effort; identify the certification authority (CA) and the DAA; and document the necessary security requirements for C&A. Ends with a documented agreement, between the program manager, the DAA, the CA, and the user representative of the approach and the results of the phase 1 Activities.

**Phase 2, Verification**
Activities to verify compliance of the system with previously agreed security requirements.

**Phase 3, Validation**
Activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

**Phase 4, Post Accreditation**
Activities to monitor system management and operation to ensure an acceptable level of residual risk is preserved. Security management, change management, and periodic compliance validation reviews are conducted.

# Level of Information System Interoperability (LISI) Profile

**The LISI Survey focuses on the four interoperability attributes:**

**Procedures, Applications, Infrastructure, and Data**

| *Nature of Operational Information Interaction* | Corresponding Computing Environment | *Level Code* | *Implications* P | A | I | D |
|---|---|---|---|---|---|---|
| Cross-Domain Interactive Manipulation | *Universal* | 4 | Enterprise Level | Interactive | Multiple Topologies | Enterprise Model |
| Shared Applications & Databases | Integrated | 3 | Domain Level | Groupware | World Wide Networks | Domain Model |
| Complex Media Exchange | Distributed | 2 | Program Level | Desktop Automation | Local Networks | Program Model |
| Simple Electronic Exchange | Connected | 1 | Local/Site Level | Standard System Drivers | Simple Connection | Local |
| Manual Gateway | Isolated | 0 | Access Control | N/A | Independent | Private |

# Summary

- This pamphlet provides a basic explanation of the the various products inc
in the development of the NR-KPP.

- CDDs, CPDs, CRDs, and ISP documents must include a NR-KPP. The NR-K
consists of the following products:

  -- Integrated Architecture Products
  -- Compliance with Key Interface Profiles (KIPs)
  -- Compliance with Information Assurance (IA) Certification/Accreditat
  -- Compliance with Net Centric Operations and Warfare Reference Mo

- The LISI Profile is an addition tool available to assess the level of a system
Interoperability

- It is hoped that this information will be of assistance to Combatant Comma
and DOD Agency's NR-KPP developers.